INSTRUCTIONS ON IMPLEMENTING THE DNSSEC SECURITY PROTOCOL FOR ".ES" DOMAIN NAMES

Additional provision number sixteen of Law 9/2014 of 9 May, The Telecommunications Act grants the public company Red.es the right to manage registration for domain names with the country code for Spain (.es).

On 21 October 2004, the Chairman of Red.es modified the instructions published on 18 July 2003, which detailed all the procedures related to assigning and registering ".es." domain names. The aim of modifying the instructions was to adapt them to the legal procedures for registering ".es" domain names, and bring them into line with the provisions of ORDER CTE/662/2003, of 18 March, which establishes the National Domain Name Plan and assigns the code ".es" to Spain.

Subsequently, on 1 June 2005, the new National Domain Name Plan came into force with the ".es" country code assigned to Spain, as approved by ORDER ITC/1542/2005, of 19 May. This regulation simplified and relaxed the requirements for assigning ".es" domain names, and also established that the Plan should be complemented by procedural guidelines drawn up by the Chairman of Red.es, by virtue of additional provision number eighteen of Law 14/2000, of 29 December, the Fiscal, Administrative and Social Measures Act, which was modified by Article 70 of Law 24/2001, of 27 December, on Fiscal, Administrative and Social Order Measures.

The Chairman of Red.es has the authority to establish the procedures for assigning domain names and other operations associated with registering domain names and internet addresses with the Spanish country code ".es", in accordance with provision number 18 of Law 14/2000, of 29 December, the Fiscal, Administrative and Social Order Measures Act, modified by Article 70 of Law 24/2001, of 27 December 2001, on Fiscal, Administrative and Social Order Measures, and in accordance with the additional provision number six of Law 34/2002, of 11 July, the Information Society Services and Electronic Commerce Act, and Order ITC/1542/2005, of 19 May, which approved the National Domain Name Plan (hereinafter, the "Domain Name Plan"), assigning the ".es" country code to Spain.

The Chairman of Red.es, in accordance with the second paragraph of article 7 of Royal Decree 164/2002, of 8 February which approves the Company By-laws of the Red.es, delegated the power to establish procedures relating to assigning domain names and internet addresses with the Spanish country code, ".es", to the General Director of Red.es, via the resolution of 21 October 2005.

In accordance with the foregoing, and while drawing up the specified regulation and procedures established in the Domain Name Plan, the General Director of Red.es ordered, on 2 January 2010, for instructions to be drawn up on the applicable procedures for assigning domain names and similar operations related to registering ".es" domain names (hereinafter the "instructions for procedures for ".es" domain names"). The aforementioned instructions for procedures for ".es" domain names are the current guidelines regulating all the procedures associated with the registration, maintenance and management of ".es" domain names.

DNSSEC is a new service associated with ".es" domain names and it enhances the security provided by the DNS (*Domain Name System*), guaranteeing the authenticity

and integrity of the data associated with the same, in order to resolve any previous vulnerability issues by using the new security protocol.

Red.es will make DNSSEC available to users of ".es" domains, and the company is responsible for developing and implementing the same in the Register. This implementation requires certain specific regulations, which is the reason why the present instructions have been drawn up.

The present instructions are written with the aim of regulating the implementation of the new security protocol DNSSEC (*Domain Name System Security Extensions*) when managing ".es" domain names, and by virtue of the powers delegated to the General Director of Red.es as referenced above, the instructions were drawn up in accordance with the guidelines established by the international community Internet Engineering Task Force (hereinafter, "IETF") in the RFC (*Request for Comments*) document 6851 "A Framework for DNSSEC Policies and DNSSEC Practice Statements", which includes a detailed list of all the technical aspects and considerations to take into account when implementing DNSSEC security protocols.

These instructions will be effective as from the date indicated by Red.es on the Registry's website, at least FIFTEEN CALENDAR DAYS in advance.

César Miralles Cabrera
General Director of the Public Company Red.es

One.- Purpose

The aim of the present instructions is to regulate the DNSSEC security protocol (hereinafter the DNSSEC service") for ".es" domain names.

For the purposes of these instructions, the manager of the DNSSEC service associated with a domain name (hereinafter the "User Manager"), is the designated Technical Contact for said domain name. Notwithstanding the foregoing, in the event that technical issues related to the domain name are managed directly by the Owner or Administrative Contact, they will have the status of User Manager.

Two.- Custody and generating the necessary keys to use DNSSEC

In order to guarantee that the DNSSEC service works for a domain name, Red.es should be provided with the necessary keys to activate the service (hereinafter, the "DS keys"), as well as the necessary information to activate the service, under the terms and conditions detailed in the technical guidelines set forth for this purpose and published on the Registry website. The User Manager is responsible for providing Red.es with these keys via the electronic means designated by the organisation, he is likewise is also responsible for their management, custody and maintenance. The User Manager also has the possibility of adding, deleting or updating the aforementioned keys at any time.

Red.es will not test whether or not the keys provided comply with technical regulations, and therefore cannot be held liable for any possible incidents caused by inadequate management of the same that prevents the DNSSEC from running correctly.

Three.- Changes to the provision of the DNSSEC service

Any modification to the DNS data associated with a domain name that uses the DNSSEC service should be carried out in such a way that it guarantees the continued operation of the domain name, which will always include, where necessary, the need to delete the DS keys in advance.

When transferring domain names that do not have the DNSSEC service activated, accredited registrars are required to collaborate in order to ensure the continued operation of the domain name being transferred.

Under no circumstances will the Assigning Authority be deemed responsible for any incidents caused by the User Manager or accredited registrars while modifying the DNS data associated with a domain name using the DNSSEC service.

Four.- Additional obligations of accredited registrars when providing the DNSSEC service

Accredited registrars that offer the DNSSEC service to their customers should make sure they are informed, before contracting the service, of the characteristics of said service. The relevant information relating to the DNSSEC service should be available in a specific additional ANNEX, which will be included in the Accredited Registrar Contract with the domain name beneficiary.